Creating a Security Awareness Program that Sticks

A Security Innovation Whitepaper

Lisa Parcella
Director of Product Management

Be Your Own Solution: Educate Your Employees

Did you know

Types of Breaches:

- Malicious attacks make up 37%
- System bugs make up 24%
- Careless insiders make up 39%

Let's face it – someone out there wants your sensitive data.

Smishing. Spear Phishing. Clickjacking. We are bombarded everyday with headlines shouting the new and inventive ways attackers are coming after our sensitive information and the catastrophic consequences when they actually get their hands on it. By now, security education should be a top priority for any organization with information to protect, which is EVERY organization. Technology is a credible line of defense, but it cannot be the only one. Your employees need to know how they can help protect your company's sensitive data and be motivated by why they should care about protecting it.

Over and over again we read about breaches in the news and of the many traits these attacks share, one to remember is the fact that attackers have TIME on their side. They can spend weeks, months and even years researching your systems and patterns and testing for vulnerabilities - when the payouts of stolen data reach into the millions and billions, any time they spend is a better payday then they'll receive working a nine to five.

Another important fact to consider is that all it takes is ONE employee to click on a link, download a file, give out seemingly innocuous but potentially hazardous information on a phone call, or hold the door for the well-dressed gentleman or lady behind them whose hands are full as they enter a secure area.

Visualize your organization as a large pipe that sensitive data flows through. We can fortify this pipe with our technological innovations and protections, making sure it is ironclad and that the major junctions are securely locked down. Employees are stationed along that pipe, siphoning and adding information to that flow. Each point along the pipe where an employee contacts it is vulnerable to a crack. Whether you have 10 or 10,000 employees, each of them has the ability to crack that pipe and all it takes is one crack for information to flow out and into the wrong hands. By arming your employees with the techniques they need to properly access, manage, store and destroy sensitive data, as well as the wherewithal to recognize attacks, you will ensure the safe flow of information and the safeguarding of your organization's reputation.

Your organization relies on your everyday employees, and they are the ones who have the power to make you more or less vulnerable to attacks.

- 69% of employees send sensitive information through insecure email channels
- 60% of employees use personal accounts to send corporate information
- 63% of employees accidentally send confidential data to an unintended email address outside the workplace
- 75% of an organization's intellectual property will travel in the text of an email or as an attachment

By simply educating your employees on security best practices, you can prevent 40% of data breaches caused at organizations by careless or unwitting insiders.

When we say security best practices, we are talking about information security and privacy awareness. Specifically, ensuring that your employees are acting in a conscientious and secure manner when it comes to accessing your company's systems and data. This includes employing best practices around email, passwords, physical and travel security, mobile security and understanding how to recognize and deflect social engineering, malware and phishing attacks. One simple way to help employees keep data safe is to teach them to

be **S.O.C.I.A.L.**:

Security-Minded

Many employees (and people in general) take security for granted, making assumptions that the systems and check and balances in place at an organization are doing the job of security for them, such as spam filters and security cameras. Realizing that each individual is responsible for vigilantly protecting an organization's data and physical assets is the first step to successful security awareness.

Organized

Keeping a clean workspace and putting everything in its proper place throughout and at the end of each day will help minimize the risk of a physical or insider attack. An employee who securely disposes of confidential data, locks their computer screen and cabinets when not in use, and keeps any external media properly stored drastically minimizes risk of exposure.

Conscientious

So many attacks prey on busy employees, catching them off-guard through their inbox, browser or on the phone, hoping that their divided attention will be enough for them to mindlessly perform an action to enable an attack, whether that means clicking on a link, giving out information freely or downloading a "helpful" program. Slowing down and taking a moment to be conscientious and mindful of the actions we take in the office help keep data safe.

Inquisitive

In addition to being conscientious, it is also important to be inquisitive every time something doesn't feel quite right. When a call comes in from an unverified asking for information that is confidential, employees should always push back on the caller. When an email request, offer or correspondence comes in that doesn't seem right, employees should follow up directly with the sender and verify the email before taking any action. Finally, even something as simple as holding a door for someone should be called into question if the person in question is not prominently displaying their credentials. Ask before you Act.

Active

Now that we know how to easily recognize and deflect simple attacks, what happens when something slips through? Employees need to know the proper procedures to follow in the event of a data compromise. Make that information prominent and easy to follow to help encourage employees to actively and quickly report any breaches or suspected attacks.

Level-Headed

With all of the touchpoints coming in and going out of a company each day through physical and technological means, it is inevitable that attacks are going to happen. When they do, employees should feel comfortable enough recognizing the attacks and how to properly respond and escalate issues without falling apart. Properly educating employees allows them to approach these situations, which can be stressful, in a calm manner from a place of assurance.

5 Ways to Create A Successful Security Education Program

Creating a successful security education program doesn't have to cost millions or take an entire team to implement. By following a few simple guidelines and choosing a vendor like Security Innovation who will work as a true partner to help you meet your security goals, any size organization can have their staff trained and acting with security in mind.

1 Stay In-Line

Tie program objectives to corporate goals. This is a step that is often overlooked when organizations try to roll-out a new program. Too many times, a new initiative is implemented and leaders are surprised when it is not immediately adopted by the masses. While it may sound a bit obvious, it is worth stating here: Just because leadership has been working tirelessly behind the scenes to procure and stand up a security education program (or any new initiative), everyone else in the organization is seeing it for the first time as if it has appeared out of thin air! This can be easily remedied by tying the program objectives to larger corporate goals that everyone is already aware of.

On a meta-level, many companies can say that one of these terms: Trust, Integrity and Brand Recognition factor among the goals of a company, or are part of a vision or mission statement. Sending out some pre-program communications about how security education helps a company meet these goals (and it helps them to maintain all three), helps users connect the dots and understand why it is important to the company that everyone participate.

2 Entice Employees

Tie program objectives to personal gains. Let's face it, we may have the most loyal employees in the world, but no matter how loyal they are to our company goals, they are even more motivated when we can tie the work that they are doing during the day to how it can benefit them in their personal lives. "What's in it for me?" is a question that marketers and communicators ask again and again for a reason - it's an important question that employees are asking themselves each time they are asked to make a decision as to what to prioritize among the many tasks given to them each day. When it comes to security education, specifically around information security and privacy, the "What's in it for me?" is a no-brainer. All of the concepts being presented help them keep their identity, financial stability, and personal liability protected. To strengthen adoption and retention rates if organizations make an effort to draw those lines for employees and show them how the security best practices they learn at work can be taken home and applied in their personal lives.

3 Inform

Create a steady drumbeat of information. Along with tying a security education program in with corporate goals and personal objectives, it is important that the program communication not stop abruptly with the rollout of training modules. By creating a steady drumbeat of information before, during and after any formal training, you accomplish a number of goals:

- Not everyone learns the same way, so by incorporating articles, blog posts, emails, tip sheets, posters and infographics along with formal training modules, you provide a range of educational materials that speak to the various learning styles of your employees *(continued)*

3 Inform *(continued)*

- By distributing different types of information at various intervals throughout the training campaign, you maximize your reach, attracting the attention of your employees at various times and in various settings, allowing them to learn about a specific security education topic through multiple avenues and perspectives, thus increasing impact and uptake

- Visual aids such as tip sheets, posters and infographics can present otherwise less engaging material in a new and interesting way

4 Promote Ongoing Communication

Get everyone involved!

Employees value face-to-face communications over any other form of communication. When rolling out a security education program, it is important to get leadership involved at every level. Some leadership touch points that help promote ongoing communication and employee interaction include:

- Have your Chief Security/Information Officer or whomever is in charge of Security/IT host a weekly or monthly Q&A online to field work- and home-based information security questions. Such an outlet encourages employees to publicize their concerns and makes the process of remediating security issues more collaborative and less clandestine and punitive.

- Use communications materials or training completion deadlines as an excuse for managers to communicate with their direct reports in small groups. This can be integrated into standing staff meetings or a special time can be set aside. No matter when these meetings take place, the goal is to create an open dialogue between managers and direct reports to help both sides understand how well the security education program is working, what lingering questions employees may have, and if the program is being effective at all. Taking even 10 minutes out of a standing staff meeting to talk about this subject will promote understanding, show employees that leaders care about the program, and help create an honest dialogue that should create proof points to map at higher organizational levels.

5 Recognize and Reward

Recognize employees for the right behaviors.

The goal of a security education program is teaching employees how to act in a secure manner so that they are protecting sensitive organizational data with vigilance at all times. This means always having a clean desk, disposing of sensitive materials in a timely and proper manner, never holding the door for a stranger, maintaining complex passwords for every system and never writing them down - the list of security demands we place on our employees goes on and on. So when our employees have mastered all that we have asked of them, it is important that we let them know that we appreciate what they are doing. Here are a couple of ways we can show that appreciation, with or, more commonly, without a rewards budget:

- Carve out a small corner of your CSO/CIO/IT website to recognize individuals on a monthly basis who are keeping your organization secure. Managers in different departments can send along a list each month with a few names of folks who they observe as acting in a secure manner and this list can be posted for a simple way of acknowledging their secure actions.

- Stockpile a closet with low-cost gratuities. These can be extras from tradeshows, vouchers for a free coffee or meal in the work cafeteria, or small denomination gift cards from local businesses. Assign a group of individuals from within the organization to watch out for employees acting in a secure fashion. When they see an individual acting securely, they can leave a redemption card at their workstation, entitling the employee to turn the card in for a gratuity.

- For a larger program, combine completing training modules and secure behaviors into a more competitive environment, setting goals for different teams or departments. Those that achieve these goals can accrue points and turn those points in for larger rewards.

5 Things to Avoid While Implementing A Security Education Program

Along with the how-to implement a security education program, there are some common mistakes many organization make. Try to avoid these pitfalls wherever possible.

1 Issuing Blind Obedience

As has been stated above, too many organizations initiate security education programs (or any new initiative) without setting a proper foundation and explaining what, why or how this will benefit your employees. Without this groundwork, it is difficult to create buy-in and positive momentum for the program and once it has been rolled out, retroactive marketing can be seen as ineffective and disingenuous.

2 One and Done Mentality

Along with setting the proper context, it is important to create conversations and action around security education. Simply assuming that employees will grasp the importance of security awareness by sitting them in front of a computer and making them complete training modules is a waste of an otherwise valuable investment on the part of the organization and a waste of time for employees. Education is an ongoing process. If you are investing in the training, invest a little bit of time in continuing the conversations, contextualizing the training by showing how it is applicable and important within your organization and be open to ongoing feedback and questions from employees.

3 Waiting for Fires

Being proactive is always better than implementing security practices only AFTER there is a data breach or attack. The cost of an average data breach is in the millions, not to mention employee time to clean it up and the long-term impact on integrity and brand recognition damage that can come from a high-profile breach. Educating employees on security best practices before there is a serious incident means there may never be one and, if there is, your employees can recognize the signs and symptoms and react more quickly and aggressively to contain an attack.

4 Only Training IT Staff

Developers definitely need to know how to create secure programs in order to keep organizational and customer data safe. However, information security and privacy awareness affects EVERY employee who has access to a telephone or computer. Attacks come in all shapes and sizes, and each employee needs to know how to protect the organization and its sensitive information.

5 Not Thinking About Security Education

It seems impossible, but there are still organizations out there that do not understand the value of security education. There is money in procuring data of every kind, whether it be for identity theft, financial gain, competitive advantage or espionage. Whether it is cybercriminals or good old fashioned run of the mill con artists, it is pretty much a guarantee that the information your organization stores is valuable to someone. The bottom line is, you must teach your employees how to protect it.

Security Innovation

187 Ballardvale Street, Suite A202
Wilmington, MA 01887
P 1.978.694.1008 **F** 1.978.694.1666
www.securityinnovation.com

The Security Innovation
Security Awareness Curriculum

Malware Awareness

In this module, learners will understand the goals of malware, identify the many types of malware, and recognize how to prevent malware infection both at work and at home.

Social Engineering

In this module, learners will identify the many forms of social engineering and its potential impacts, identify techniques used by social engineers and understand how to establish validity of requests in order to perform daily business functions in light of the threat of social engineers.

Password Security

Learners will recognize the risks surrounding password security, identify safeguards used to protect passwords, and summarize techniques used by attackers to obtain passwords. In an interactive exercise, users will learn how to create and remember strong passwords, eliminating the need to turn to insecure practices.

Email Security

Learners will be taught to recognize malicious email before it can become a threat, how to properly handle email, and best practices around how and when to use email to send specific types of information.

Physical Security

This module teaches students accepted practices for minimizing breaches and gives them the ability to identify different types of data that may be exposed via hardware theft. Students will be introduced to the risks associated with transporting sensitive data and the importance of maintaining personal security while traveling.

Mobile Device Security

In this module, students will learn about mobile devices, the ways in which data can be leaked or lost, and the challenges that arise when the line of what is corporate and what is personal is blurred. This course will look at mobile device security from a number of platforms.

Phishing Awareness

Through this module, learners will recognize malicious email before it can become a threat, understand the various ways in which attackers try to trick and entice users to trigger malicious events through email, and best practices to properly handle and avoid phishing attacks.

Travel Security

With the amount of data we are able to carry around in devices as small as a pack of gum, travel security is more important than ever. This module introduces students to the risks associated with transporting sensitive data, offers guidance around how to travel safely with sensitive information and when to leave it at home, and examines the importance of maintaining personal security while traveling.

PCI Compliance

Those in the retail and ecommerce industry are required to be PCI Compliant. This course is intended to teach students to follow the PCI Security Standards in order to understand how to identify different types of sensitive data and handle it properly.

Learn About our Security Awareness Training Program

Recognized as a Leader in the Gartner Magic Quadrant for Security Awareness Training, our course program is designed to be highly interactive and includes scenario-based educational modules to equip employees with the skills to recognize the importance of being aware and to proactively protect themselves against potential information security threats.

Each module combines instruction with highly interactive games and comes with a suite of complementary communications materials, designed to enhance the learning process.